

10/561216

MODIFIED PTO/SB/08 A &amp; B (06-03)

WIPO Receipt No. 19 DEC 2005

Substitute for Form 1449 A &amp; B/PTO

INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1 Attorney Docket Number Q92077

Application Number	Not Yet Assigned
Confirmation Number	Not Yet Assigned
Filing Date	December 19, 2005
First Named Inventor	Isamu TERANISI
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned

U.S. PATENT DOCUMENTS					
Examiner Initials <sup>a</sup>	Cite No. <sup>1</sup>	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		Number	Kind Code <sup>3</sup> (if known)		
DA		US 6,081,597	A	06-27-2000	NTRU Cryptosystems, Inc. Hoffstein et al
		US			

JB  
W/M

FOREIGN PATENT DOCUMENTS						
Examiner Initials <sup>a</sup>	Cite No. <sup>1</sup>	Foreign Patent Document		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Translation <sup>6</sup>
		Country Code <sup>4</sup>	Number <sup>4</sup>			
DA		JP	2000-516733	A	12-12-2000	
DA		WO	98/08323	A1	02-26-1998	
DA		AU	4582897	A	03-06-1998	
DA		CA	2 263 588	A	01-18-2005	
DA		CN	1232588	A	10-20-1999	

NON PATENT LITERATURE DOCUMENTS					
Examiner Initials <sup>a</sup>	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city, and/or country where published.			Translation <sup>6</sup>
DA		Victor Shoup, "OAEP RECONSIDERED (Extended Abstract)," LNCS, Vol. 2139, 2001, pages 239 to 259.			
DA		Phong Q. Nguyen, et al. "ANALYSIS AND IMPROVEMENTS OF NTRU ENCRYPTION PADDINGS," LNCS, Vol. 2442, 2002, pages 210 to 225.			
DA		John A. Proos, "IMPERFECT DECRYPTION AND AN ATTACK ON THE NTRU ENCRYPTION SCHEME," University of Waterloo, January 7, 2003, pages 1 to 28.			
DA		Eliane Jaulmes, et al. "A CHosen-CIPHERTEXT ATTACK AGAINST NTRU," Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000, pages 20 to 35.			
DA		Jeffrey Hoffstein, et al. "PROTECTING NTRU AGAINST CHosen CIPHERTEXT AND REACTION ATTACKS," NTRU Cryptosystems Technical Report, Report #016, Version 1, June 9, 2000, pages 1 to 6.			
DA		Jeffrey Hoffstein, et al. "OPTIMIZATIONS FOR NTRU," NTRU Cryptosystems, Inc., pages 1 to 12. 2-000			
DA		Joseph H. Silverman, "PLAINTEXT AWARENESS AND THE NTRU PKCS," NTRU Cryptosystems Technical Report, Report #007, Version 2, June 2000, pages 1 to 7.			
DA		Don Coppersmith, et al. "LATTICE ATTACKS ON NTRU," Eurocrypt '97 Springer Lecture Notes in Computer Sciences, 1997, pages 52 to 61.			
DA		Jeffrey Hoffstein, et al. "NTRU: A RING-BASED PUBLIC KEY CRYPTOSYSTEM". 1998			

Examiner Signature	Jamli J. Farani	Date Considered	4/11/07
--------------------	-----------------	-----------------	---------

<sup>a</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>3</sup>See Kind Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov), MPEP 901.04 or in the comment box of this document. <sup>5</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST. 3). <sup>6</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>7</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>8</sup>Applicant is to indicate here if English language Translation is attached.